E61

Open Transaction Manager Access (OTMA) Security Considerations

Alonia (Lonnie) Coleman, IMS Advanced Technical Support

Las Vegas, NV **September 15 - September 18, 2003**

RETURN TO INDEX

Agenda

- OTMA overview
- OTMA security overview
- IMS/OTMA security levels
  - IMS/OTMA security enhancements
- OTMA Callable Interface (OTMA/CI)
- Summary

OTMA Overview

- What is OTMA?

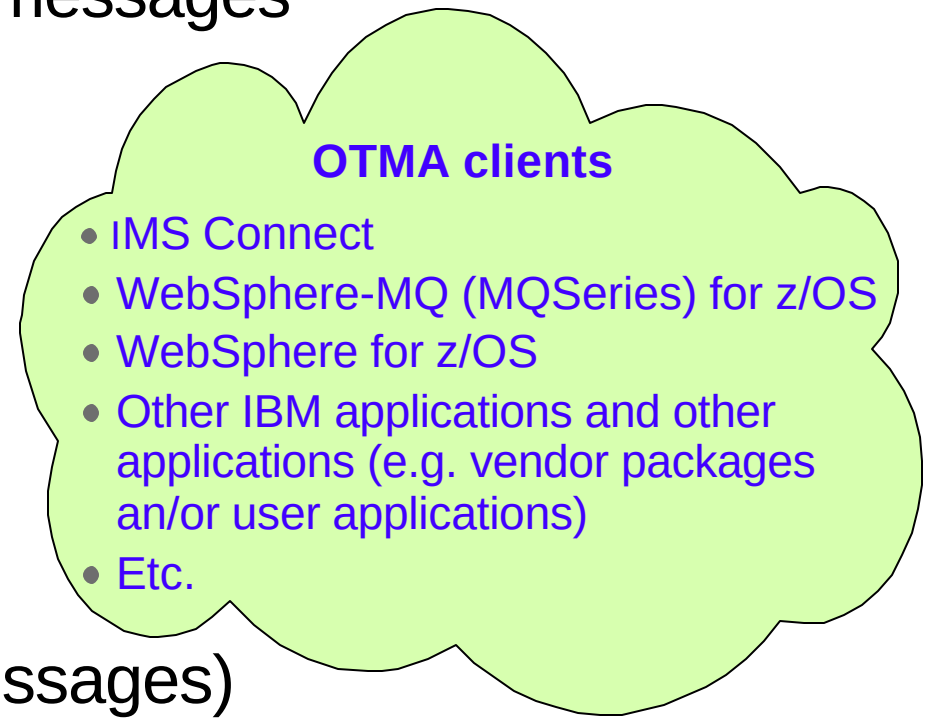
  A client-server protocol which
  - Provides ***high performance***
  - Is ***transaction-based***
  - Is ***connectionless***

  A gateway for transactions outside IMS to enter IMS

- OTMA
  - Uses MVS Cross-System Coupling Facility (XCF) services to communicate between IMS/OTMA and OTMA clients
  - Allows ***MVS programs***, called ***OTMA clients***, to access IMS commands and IMS applications

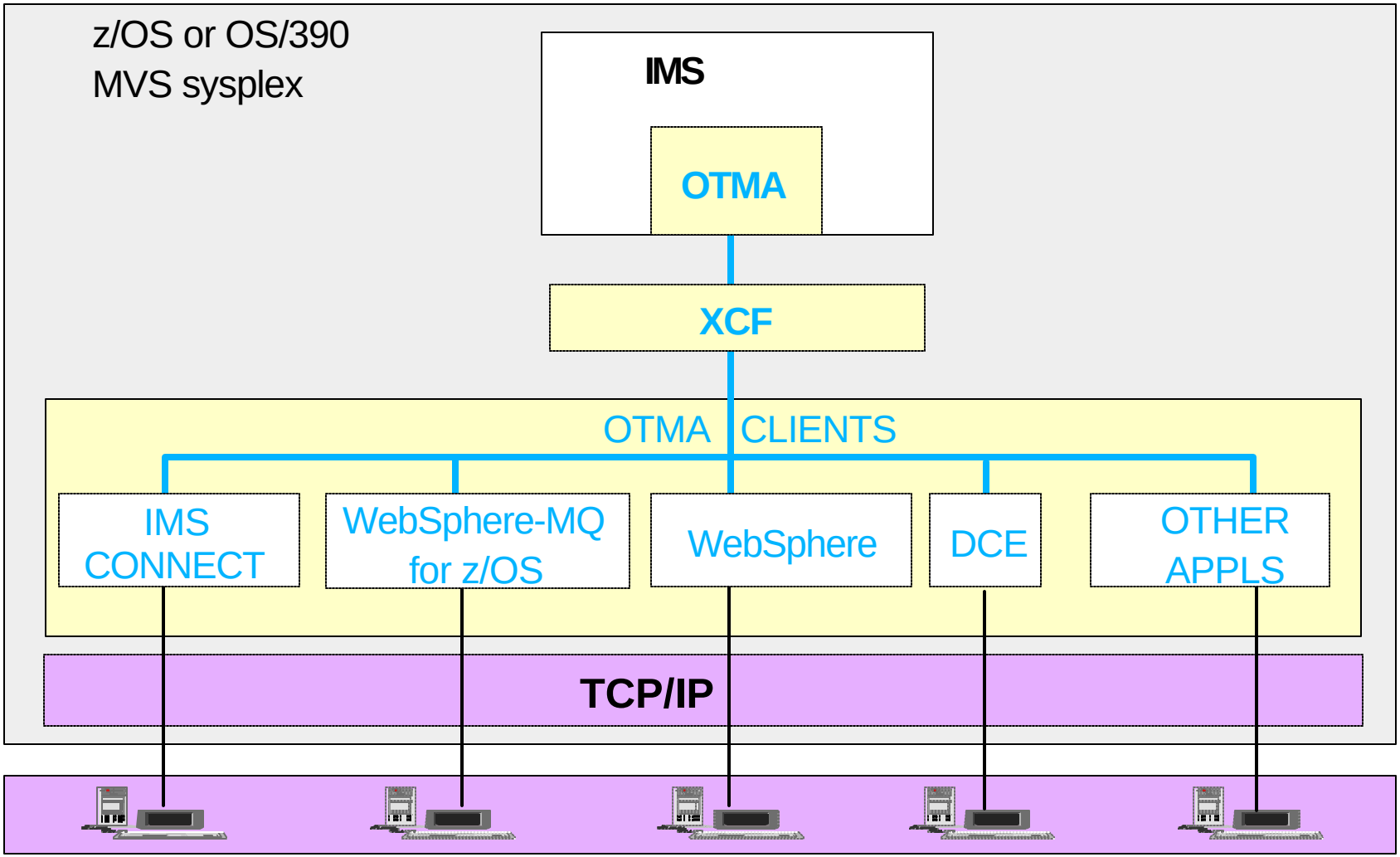
OTMA Clients (MVS Programs)

- An OTMA client may perform all of the following functions
  - Receive and transmit input messages
  - Translate messages
    - From ASCII to EBCDIC (input messages)
    - From EBCDIC to ASCII (output messages)
  - Build headers
    - OTMA headers (input messages)
    - TCP/IP headers (output messages)
  - Receive and transmit output messages



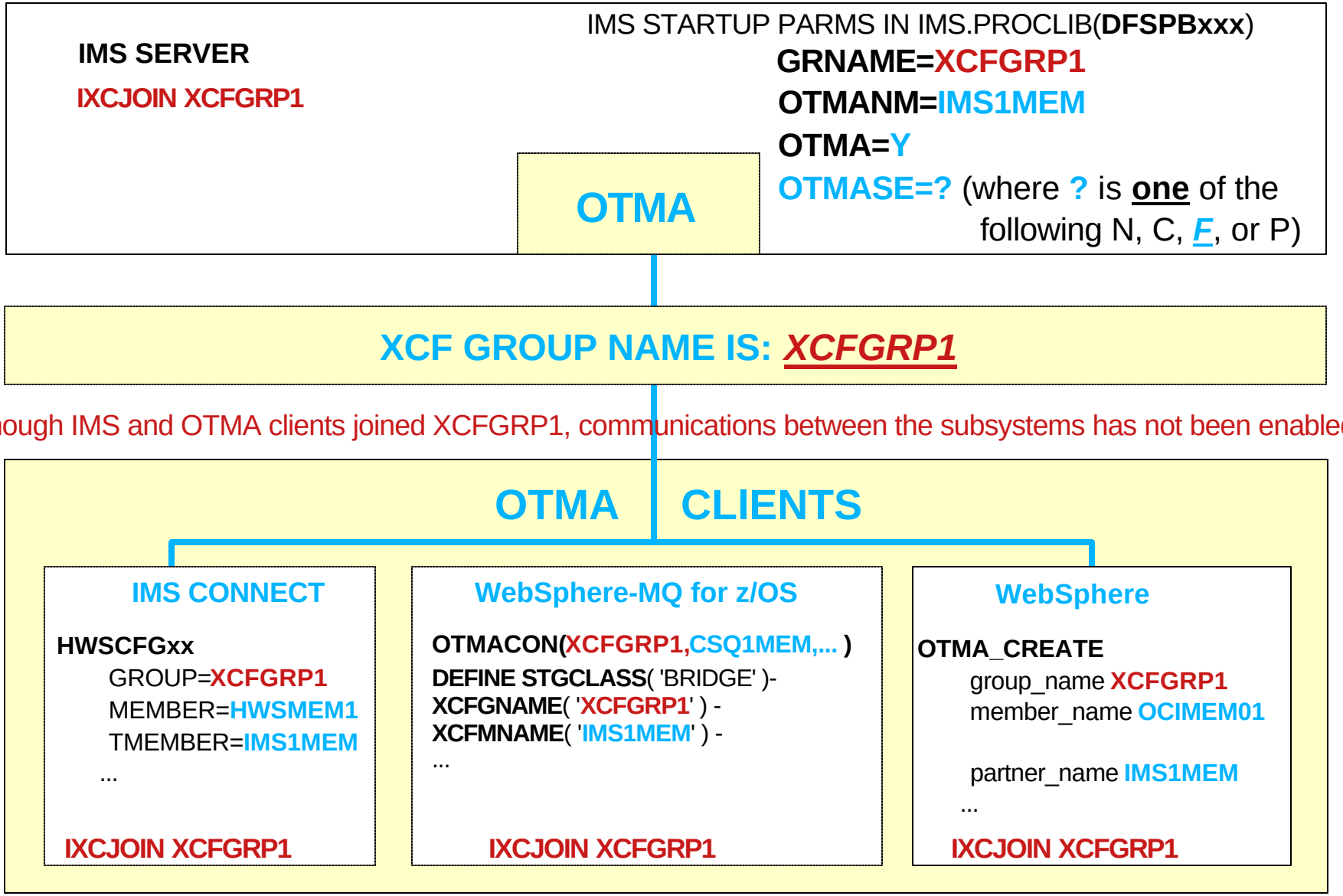
An XCF Group

An OTMA client must be a member of the ***same XCF group*** as the IMS/OTMA with which it communicates

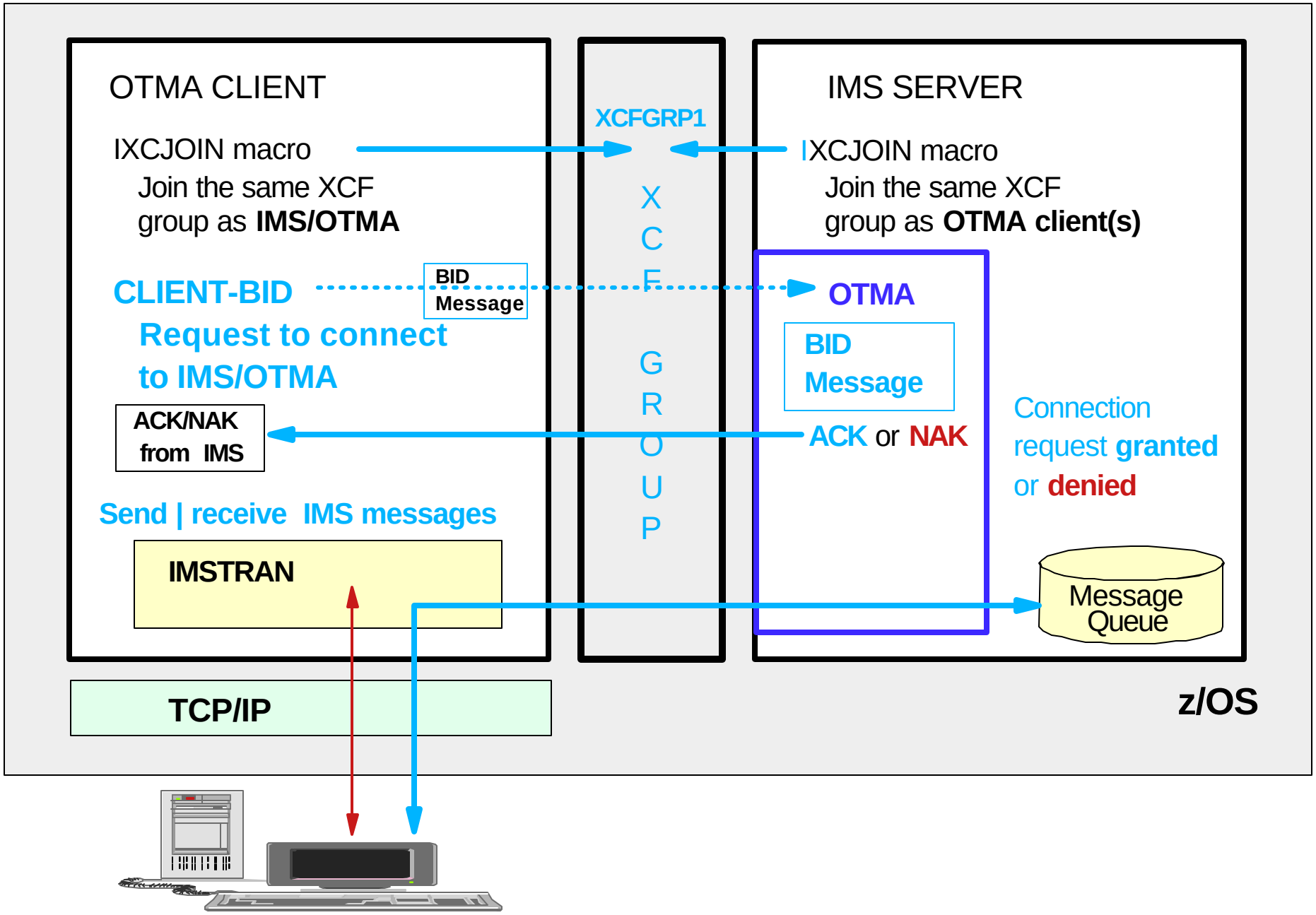


TCP/IP client server applications or terminals

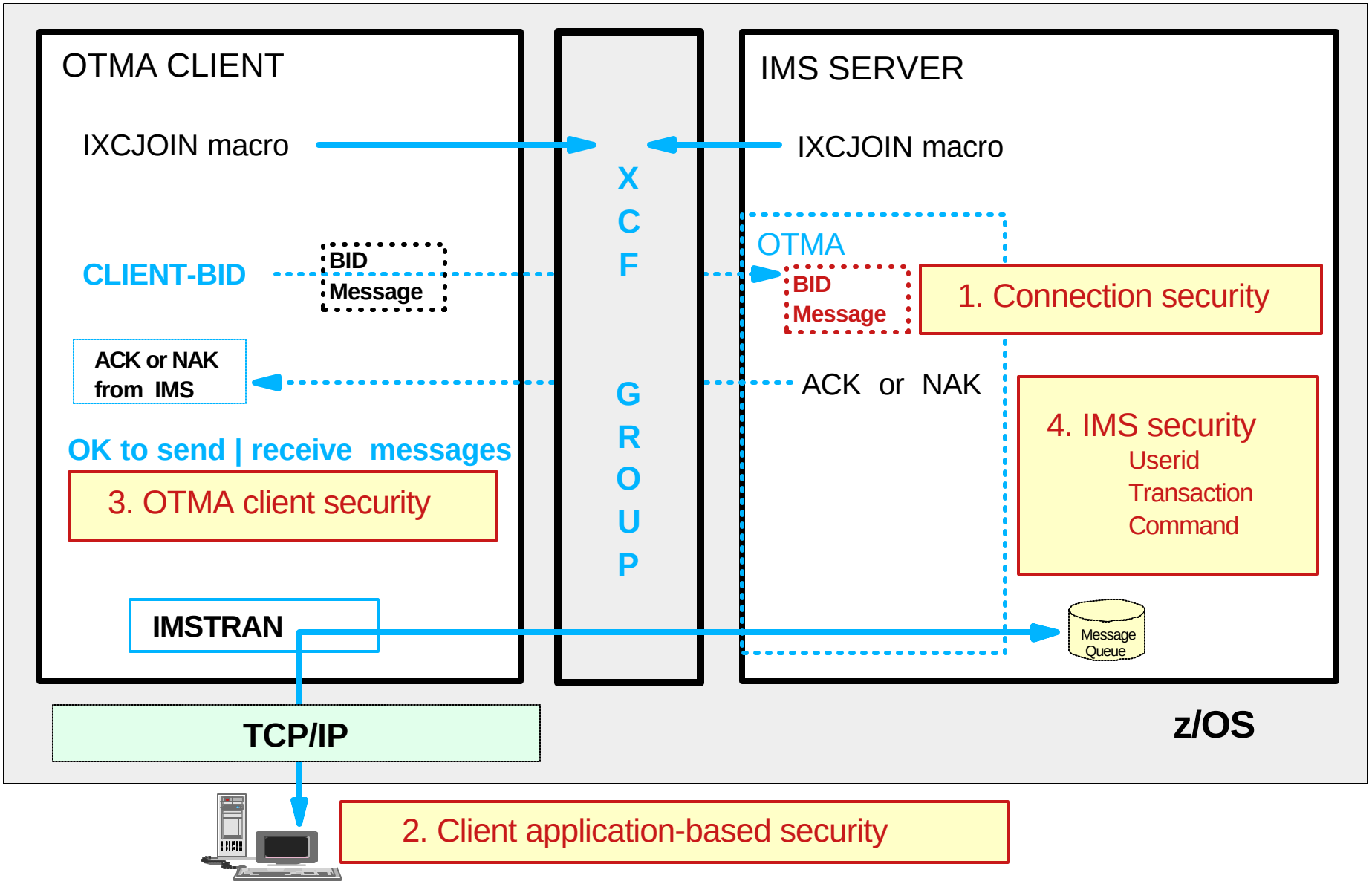
Each OTMA Client Joins the XCF Group



The Client-bid Message



End-to-End Security Options



Security Info In Messages Sent To OTMA

OTMA MESSAGE PREFIX	MESSAGE TYPE	
MESSAGE CONTROL INFORMATION (MCI)	CLIENT-BID MESSAGE	END USER TRANSACTION OR COMMAND MESSAGE
STATE DATA (SD)	..., ACEE AGING VALUE, ...	
SECURITY DATA (SE)	SECURITY FLAG (N / C / F) UTOKEN USERID (1) SAF PROFILE (1)	SECURITY FLAG (N / C / F) UTOKEN USERID (1) SAF PROFILE (1)
USER DATA		
APPLICATION DATA		IMS TRANSACTION CODE -OR- IMS COMMAND

NOTE (1). This security information is optional when message includes a UTOKEN

IMS System Programmers and DBAs

- It is important for IMS technicians to understand how OTMA security works
  - Security administrators do not understand IMS, for example

When is OTMA required (or not required) to invoke RACF?

Which security facilities (RACF and/or user exit routines) may be invoked for OTMA messages? What are the circumstances under which those security facilities are invoked (or not invoked)?

What IMS naming conventions are used to define RACF security profiles for OTMA environments?

How do IMS security options (which IMS technicians specify) affect RACF performance?

  - When an OTMA security issue is encountered YOU will be called upon to provide a solution!!

OTMA Security Overview

- OTMA security is ***optional***
- OTMA provides several security options

OTMA Security Options	Comments
1. No security checking at all	Neither RACF nor user exits are invoked
2. No RACF security checking	User exit(s) are invoked, RACF is not invoked
3. RACF security checking only	RACF is invoked, user exits are not invoked
4. RACF and user exit routines security	Both RACF and user exits are invoked

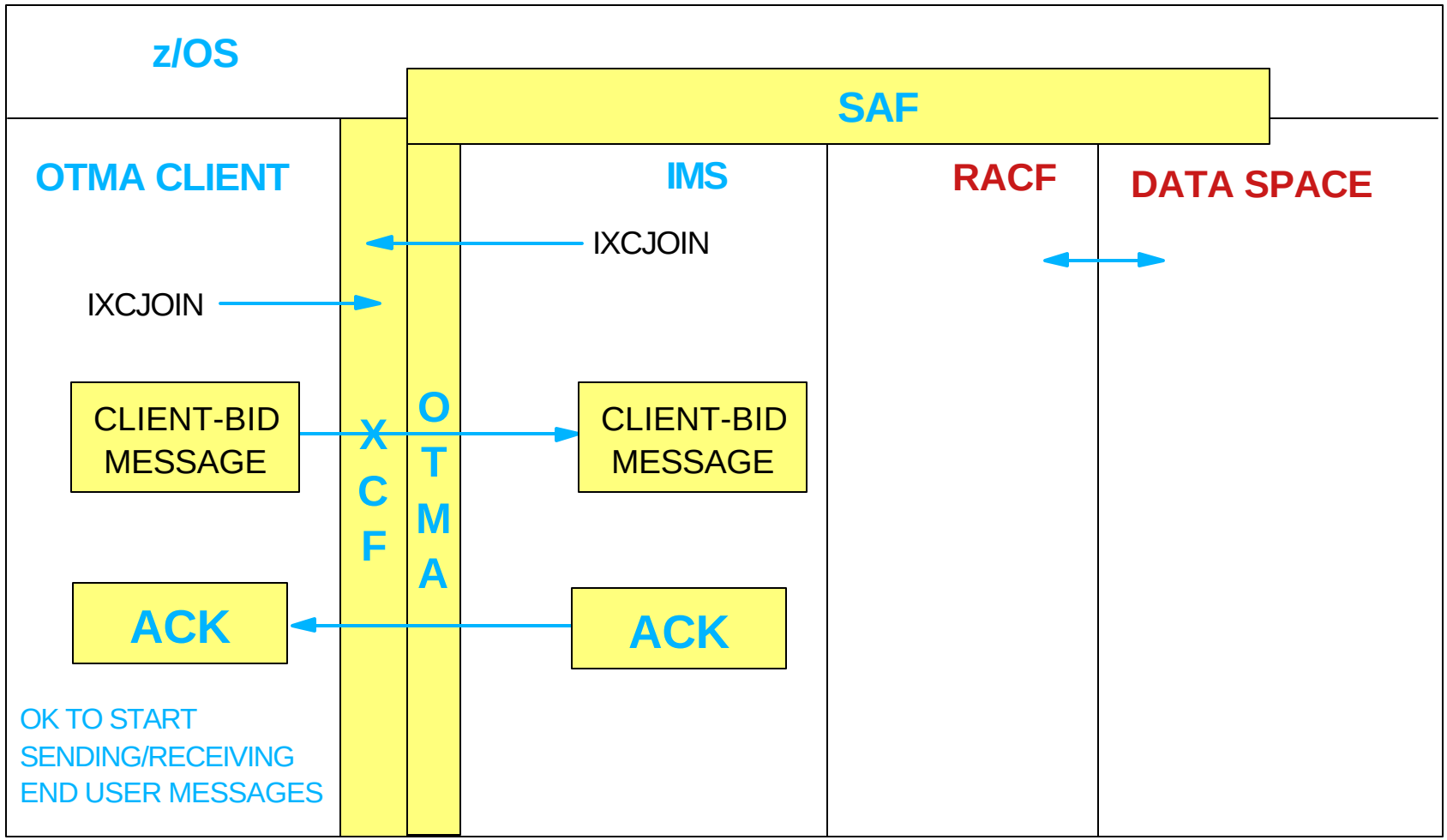
- The OTMA security level
  - Determines ***whether RACF is invoked*** to perform security checking
    - Does ***not*** affect the invocation of user exit routines
  - Is established via startup parameter or command
    - OTMASE=*x* or /SECURE OTMA *xxxxxxx*

OTMA Security Levels

- IMS-wide OTMA security levels
  - **NONE**
    - Do not invoke RACF, ACEEs are not created
  - **CHECK**
    - Invoke RACF, create an ACEE in the control region for the userid in the message
  - ***FULL*** (the default)
    - Same as CHECK, ***PLUS***
      Reverify the userid in the message when the application issues a GU (GET UNIQUE) call to retrieve the message for processing
- Message-by-message OTMA security level
  - **PROFILE**
    - Check each incoming message to determine if the security level
      - The security flag in each message one of the following: N, C, F, or P

/SEC OTMA NONE or OTMASE=N

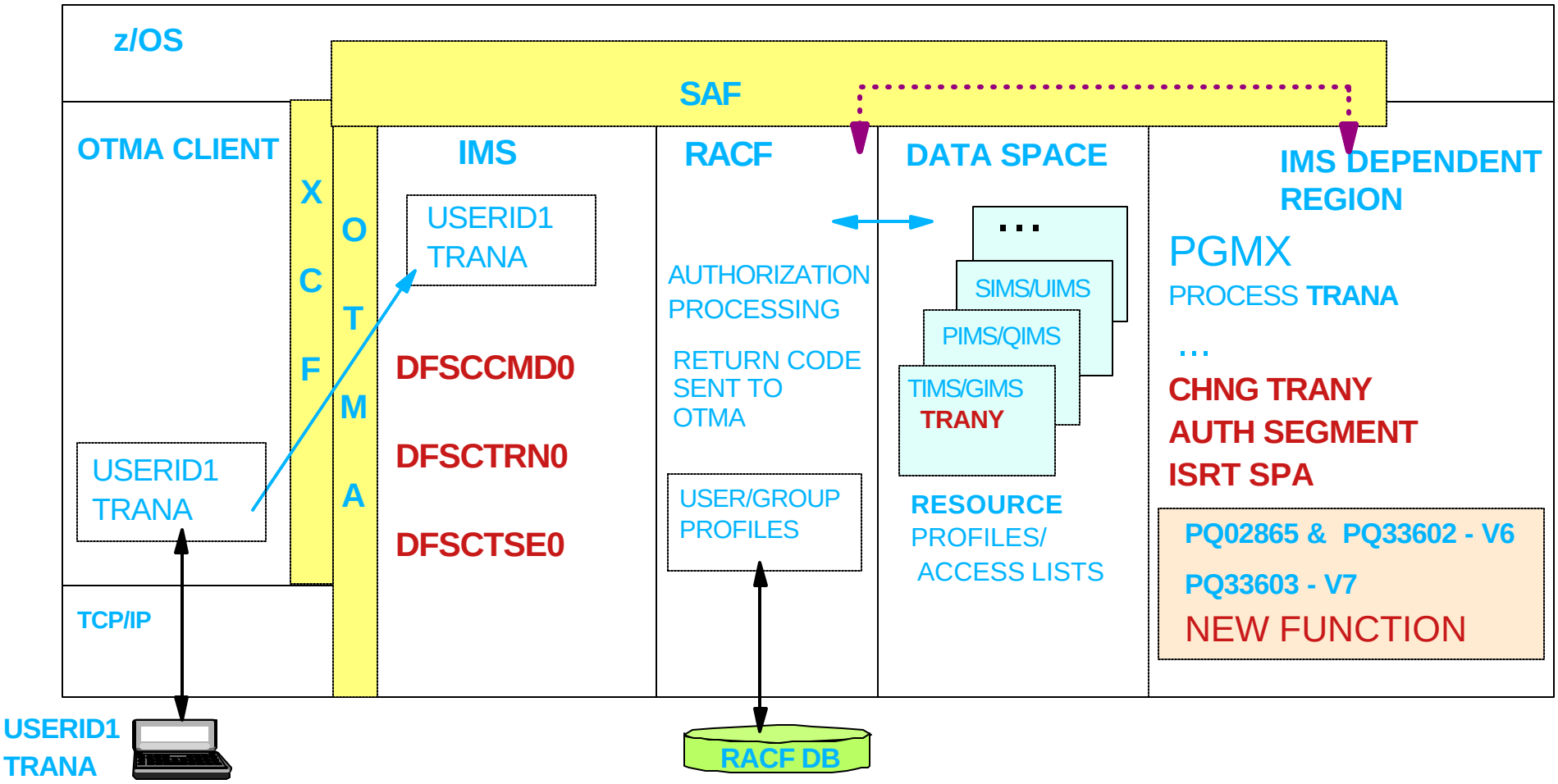
For Client-Bid Requests



RACF IS NOT CALLED BY OTMA FOR CLIENT-BID CONNECTION SECURITY CHECKING.
ALL CLIENT-BID CONNECTION REQUESTS ARE ALLOWED.
SECURITY INFO IN CLIENT-BID MESSAGE IGNORED BY OTMA.

/SEC OTMA NONE or OTMASE=N

For End User Messages



RACF IS ***NOT*** INVOKED FOR SECURITY CHECKING FOR END USER MESSAGES RECEIVED VIA OTMA(SECURITY INFORMATION IN INCOMING MESSAGES IGNORED BY OTMA)

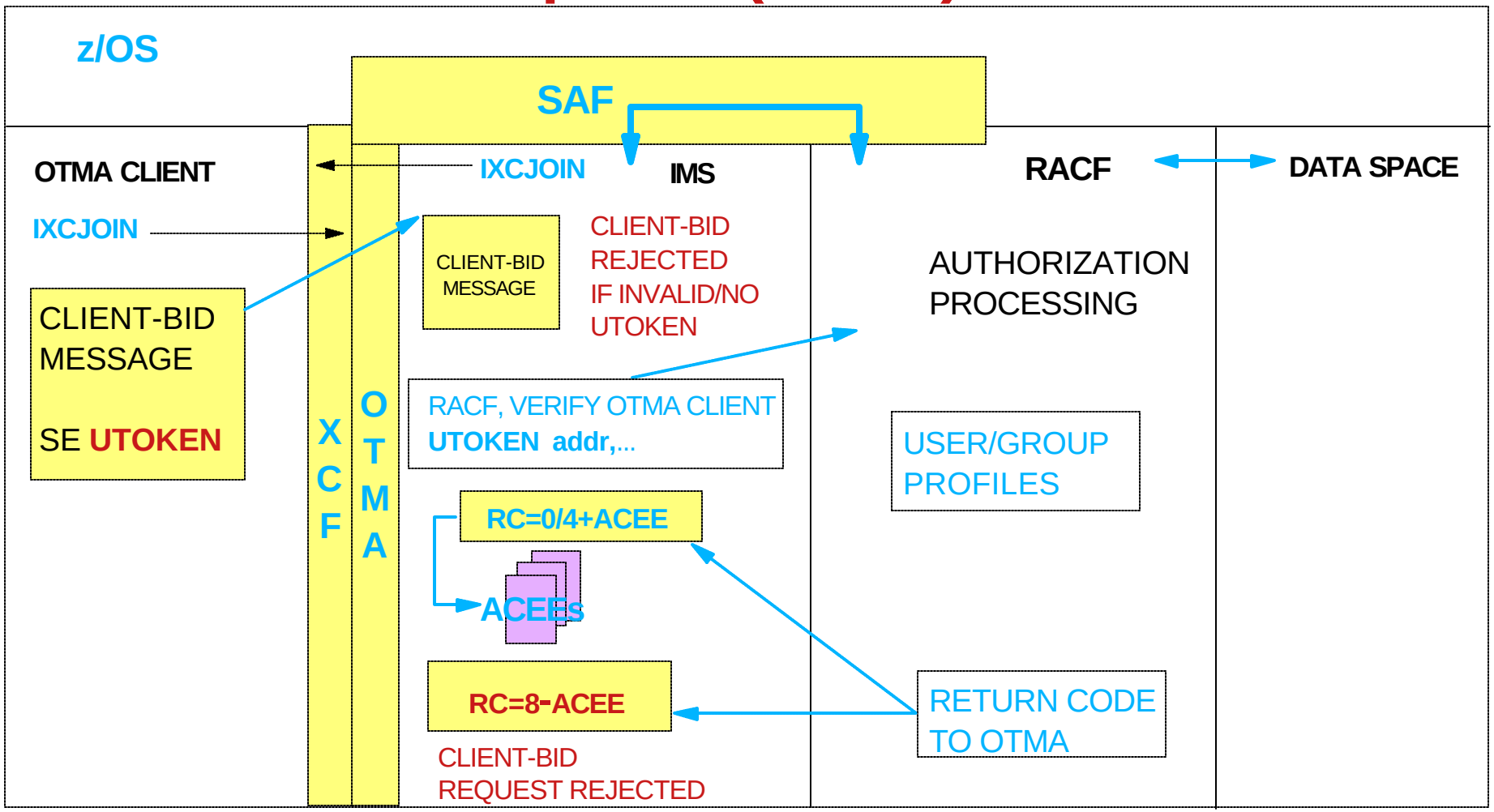
COMMANDS: **/BRO**, **/LOCK**, **/LOG**, **/RDISPLAY**, **/UNLOCK**; **DFSCCMD0** ***EXIT INVOKED***

TRANSACTIONS: RACF NOT INVOKED UNLESS APARS ARE NOT INSTALLED;

EXITS: **DFSCTRN0** AND **DFSCTSE0** EXITS ***ARE INVOKED***

/SEC OTMA CHECK or OTMASE=C

For Client-Bid Requests (Part 1)

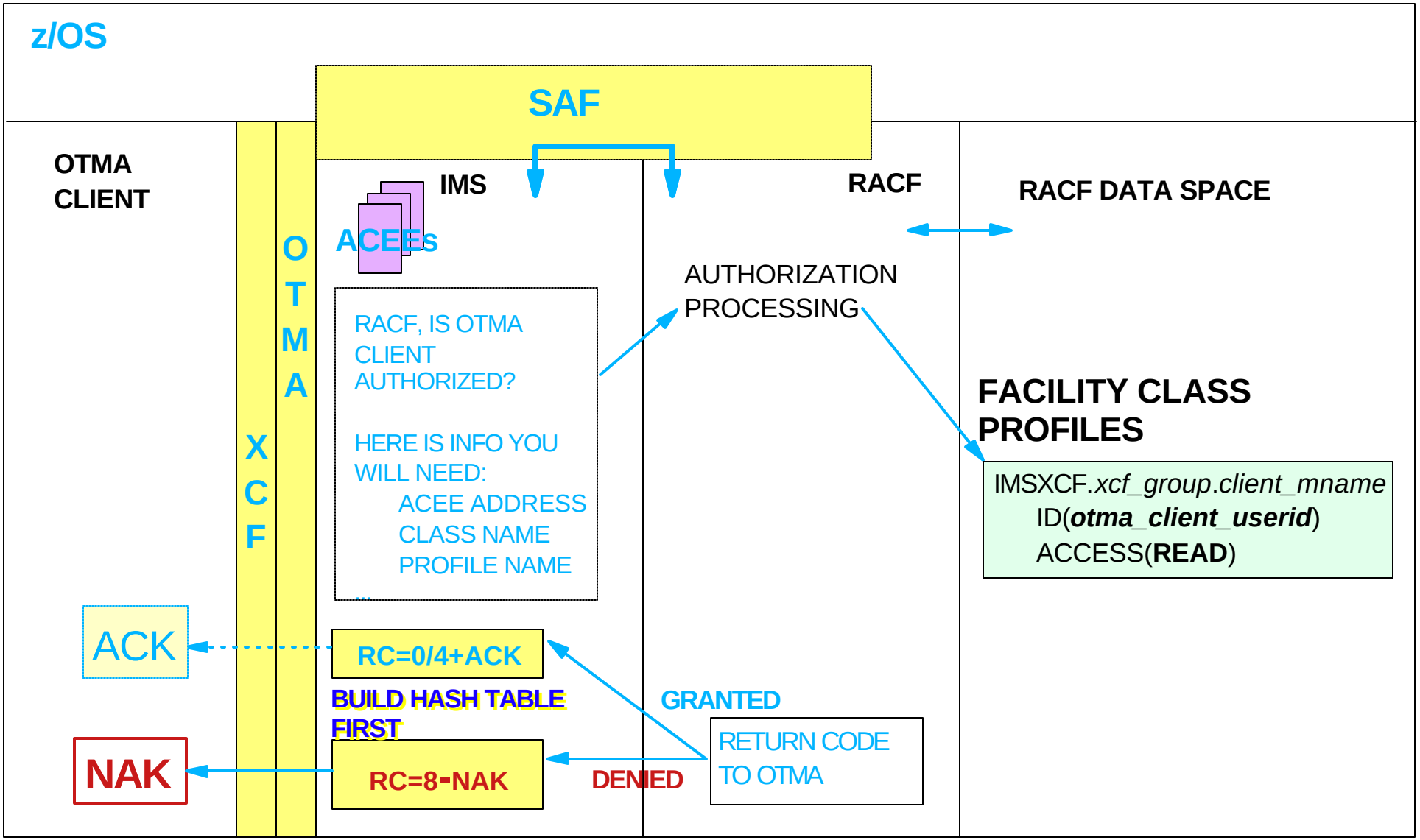


RACF ***IS*** INVOKED BY OTMA FOR CLIENT-BID CONNECTION SECURITY CHECKING:

1. TO VERIFY THAT THE SECURITY INFO IN THE ***REQUIRED*** UTOKEN IS VALID **(ELSE CLIENT-BID IS REJECTED)** AND TO RETURN AN ACEE FOR A VALIDATED OTMA CLIENT
2. TO CHECK THE APPROPRIATE FACILITY CLASS PROFILE TO DETERMINE IF THE OTMA CLIENT CAN CONNECT TO OTMA

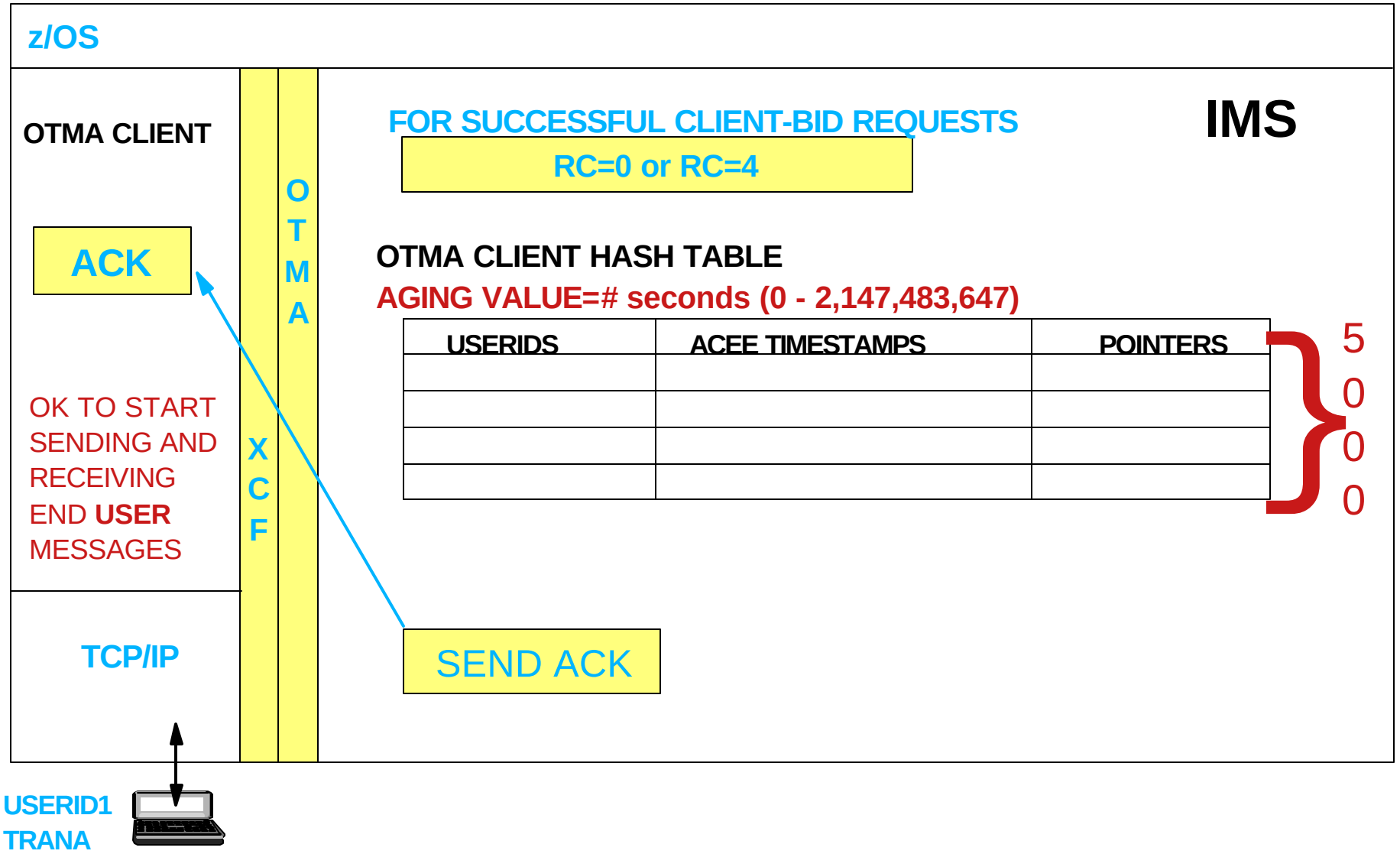
/SEC OTMA CHECK or OTMASE=C

For Client-Bid Requests (Part 2)



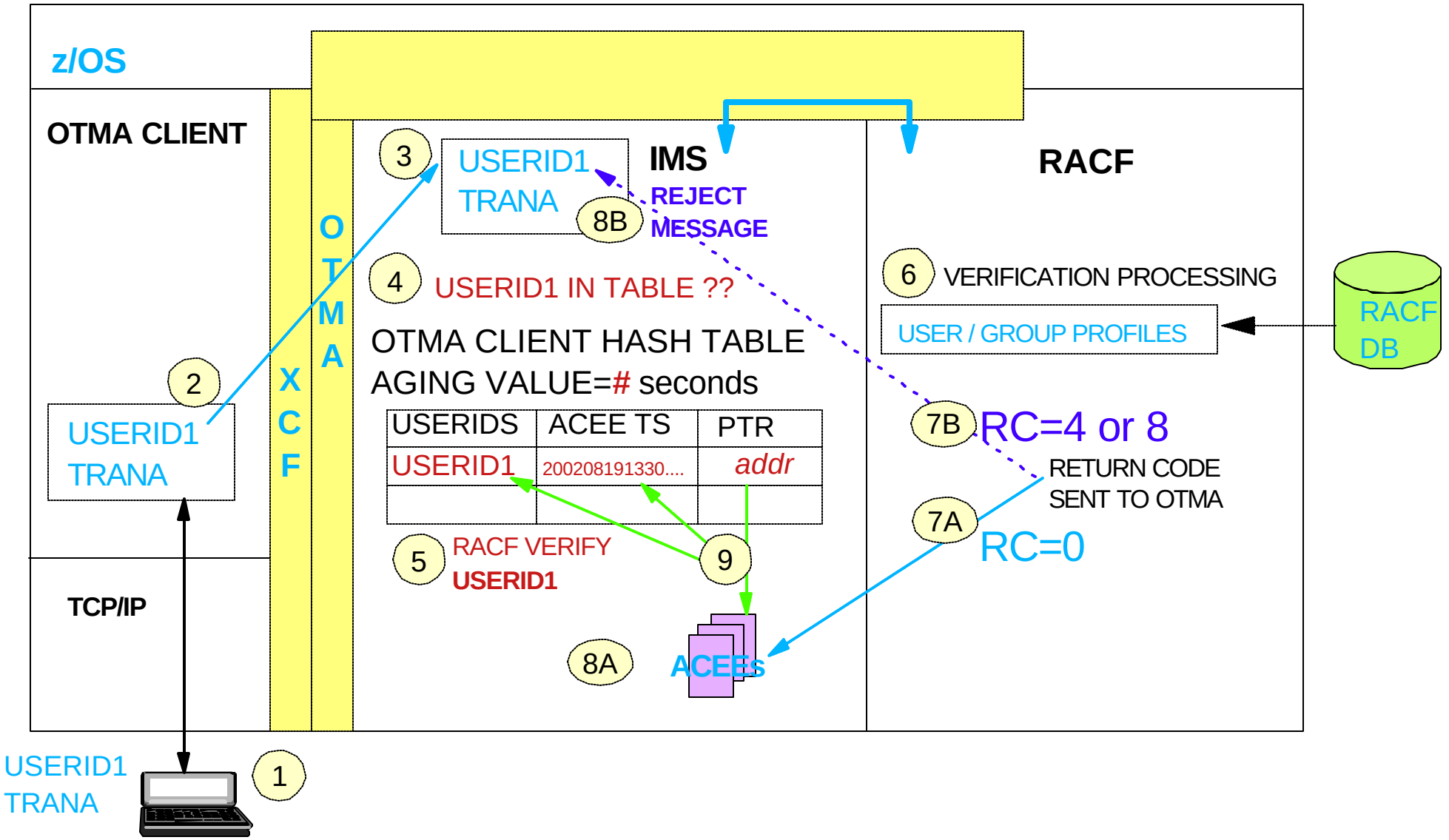
/SEC OTMA CHECK or OTMASE=C

A Successful Client-Bid (Part 3)



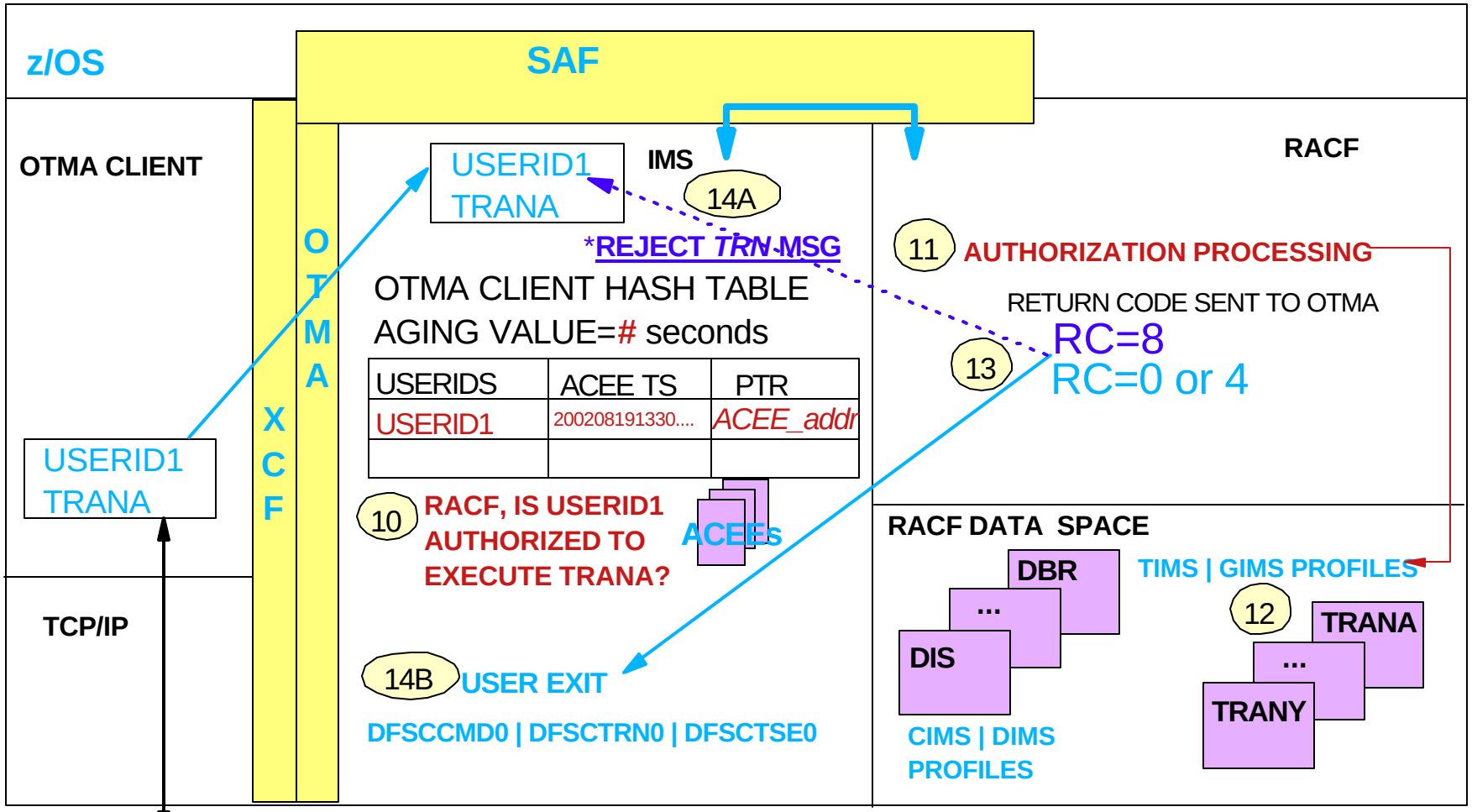
/SEC OTMA CHECK or OTMASE=C

End User Messages (Part 1A)



/SEC OTMA CHECK or OTMASE=C

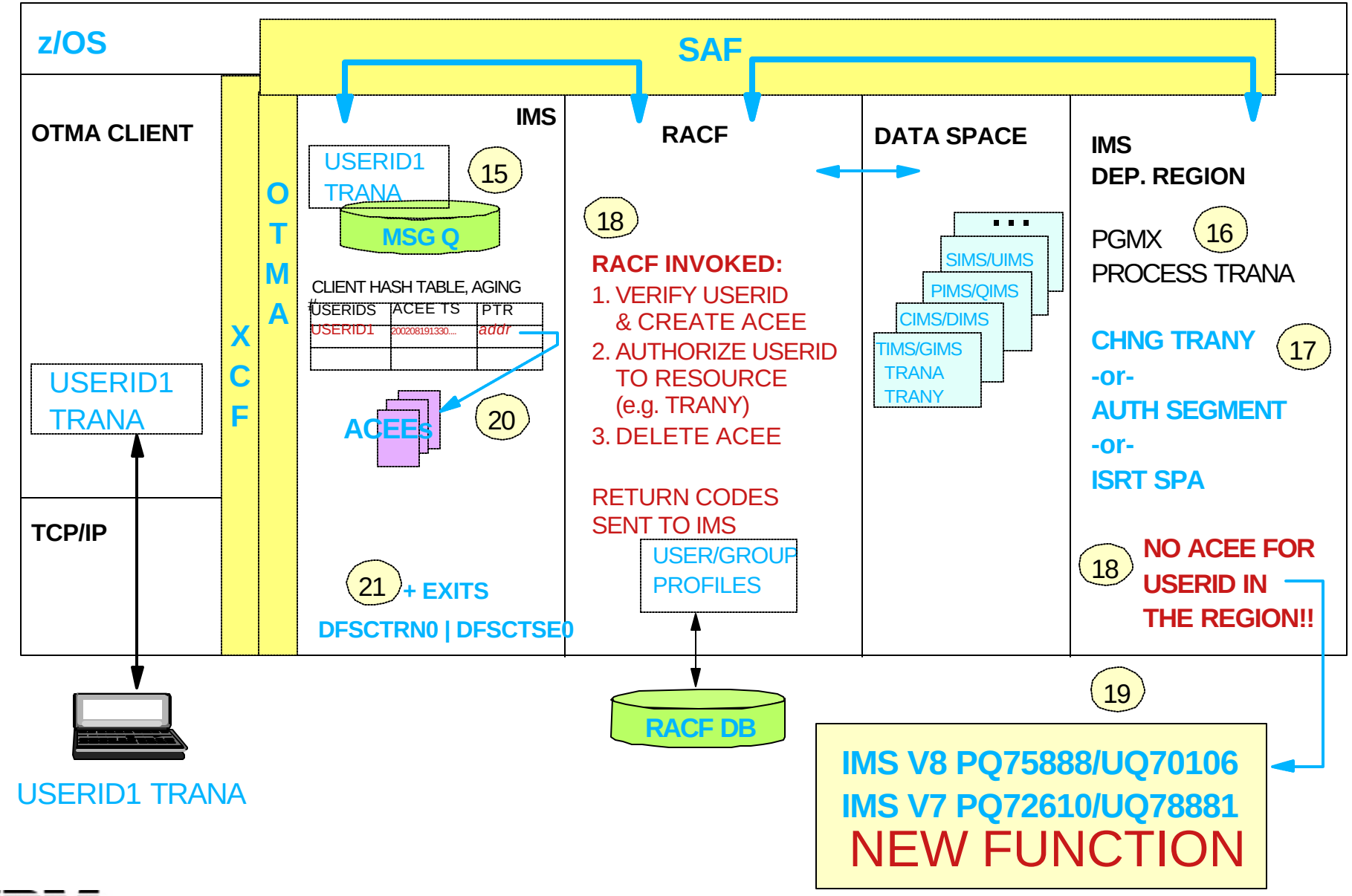
End User Messages (Part 1B)



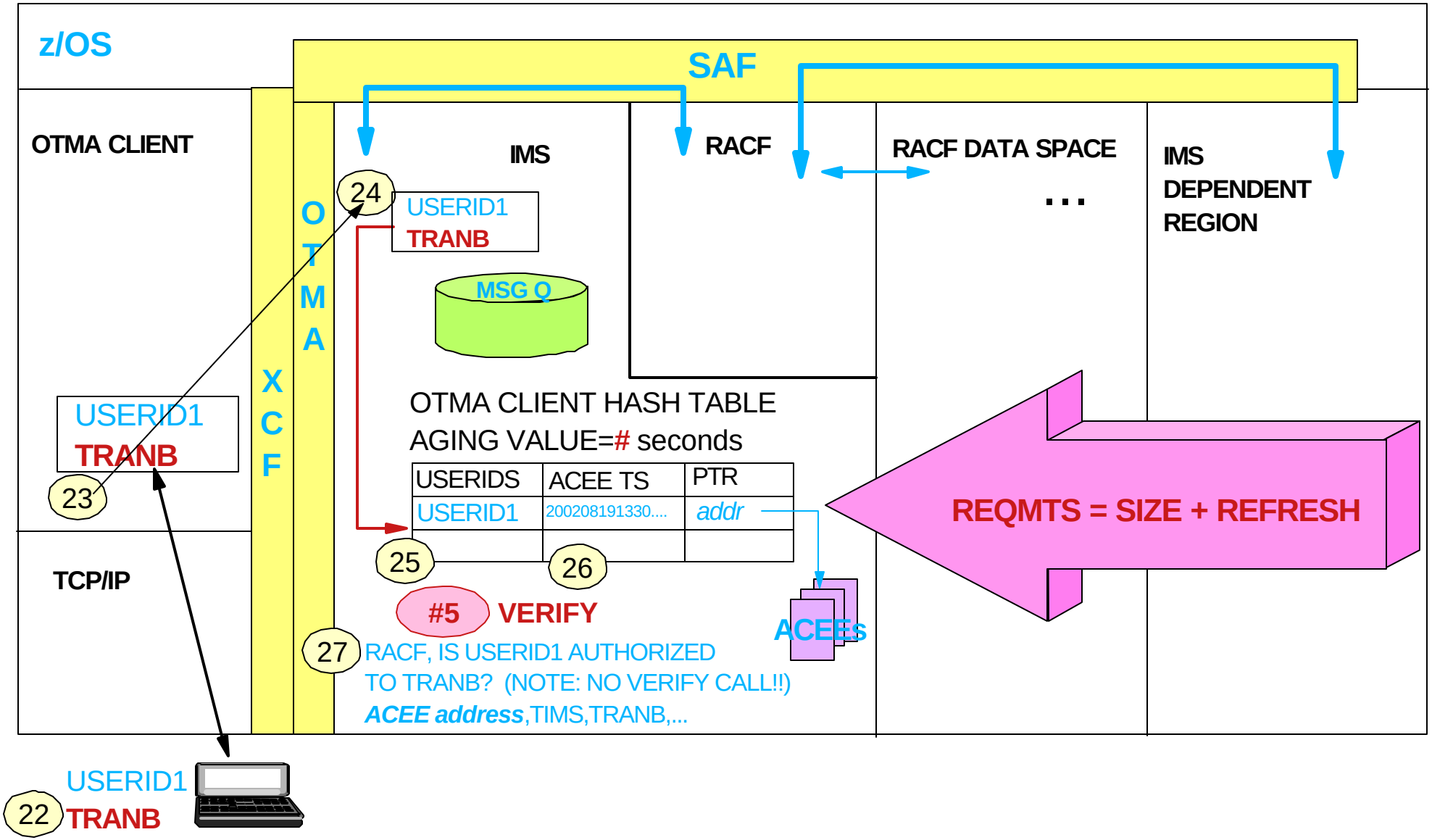
NOTE: AN OTMA MESSAGE CAN BE QUEUED FOR PROCESSING ***ONLY*** AFTER ALL SECURITY CHECKS HAVE BEEN SUCCESSFULLY PASSED.

/SEC OTMA CHECK or OTMASE=C

Processing End User Transactions



Hash Table Use



What Happens .... (1)

- When the OTMA client hash table has 5000 entries?

OTMA CLIENT HASH TABLE

AGING VALUE=# seconds (0 - 2,147,483,647)

USERIDS	ACEE TIMESTAMPS	POINTERS

5000

- Without APARs
  - Only 5000 ACEEs are cached
    - After the hash table is full, ACEE caching is not performed
    - RACF is invoked to:
      (1.) perform verification and create ACEE, (2.) perform resource authorization check, and (3.) delete ACEE

- With APARs, OTMA
  - Dynamically allocates storage to the hash table
  - Can cache over 5000 ACEEs

IMS V8 PQ75888/UQ70106
IMS V7 PQ72610/UQ78881
NEW FUNCTION

What Happens .... (2)

- When a security administrator changes information in RACF profiles
  - Changes USER and/or GROUP profiles
  - Changes USERID-to-GROUP connections
  - Changes the access list of resource profiles
    - Transaction, command, database, segment, application, etc.
- Client hash table need to be refreshed to capture the changes in ACEE(s) representing the userid(s)
  - Without APARs, you must stop/restart OTMA client or stop/restart OTMA to refresh hash table
  - With APARs

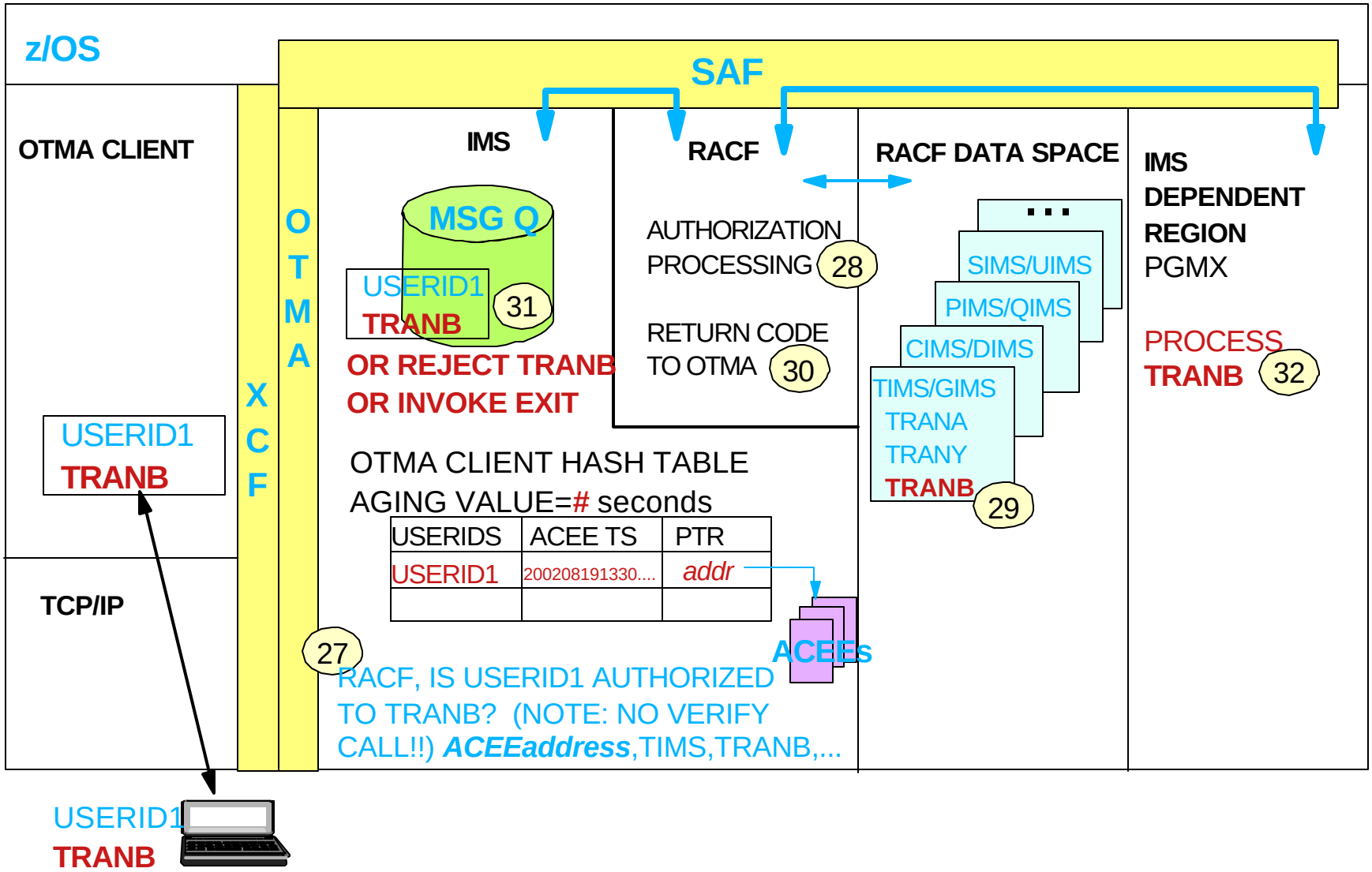
IMS V8 PQ66549
IMS V7 PQ68350
NEW FUNCTION

These APARs supply new keywords on the /SECURE command to cause the ACEEs for all OTMA clients to be refreshed or only those ACEE for a specific OTMA client.

/SECURE OTMA **REFRESH**

/SECURE OTMA REFRESH **TMEMBER <tmember name>**

Hash Table Use ...

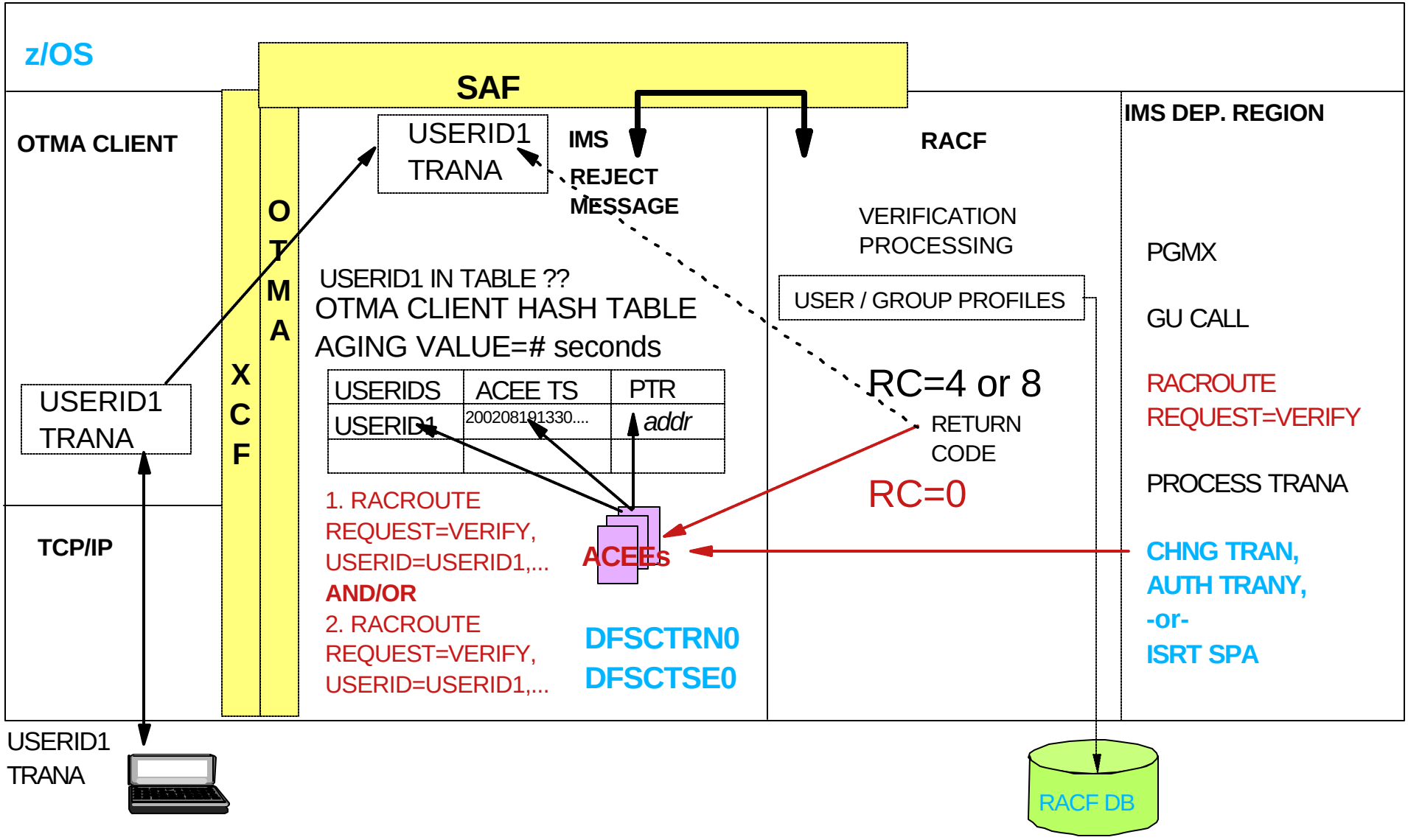


/SEC OTMA FULL or OTMASE=F

- Security checking identical to level **CHECK** for some things
  - Client-bid requests
  - IMS commands
  - Hash table use
  - User exit routines
    - Command Authorization Exit (DFSCCMD0)
    - Transaction Authorization Exit (DFSCTRN0)
    - Security Reverification Exit (DFSCTSE0)
- When the OTMA security level is **FULL**
  - RACF processing is different for IMS transactions
    - RACF is invoked to verify the userid in the message when the application program issued the **GET UNIQUE (GU)** call to retrieve the message for processing
    - ***FULL*** has some RACF overhead if application does not request transaction/data resources via CHNG and/or AUTH calls nor perform deferred conversational program message switches

/SEC OTMA FULL or OTMASE=F

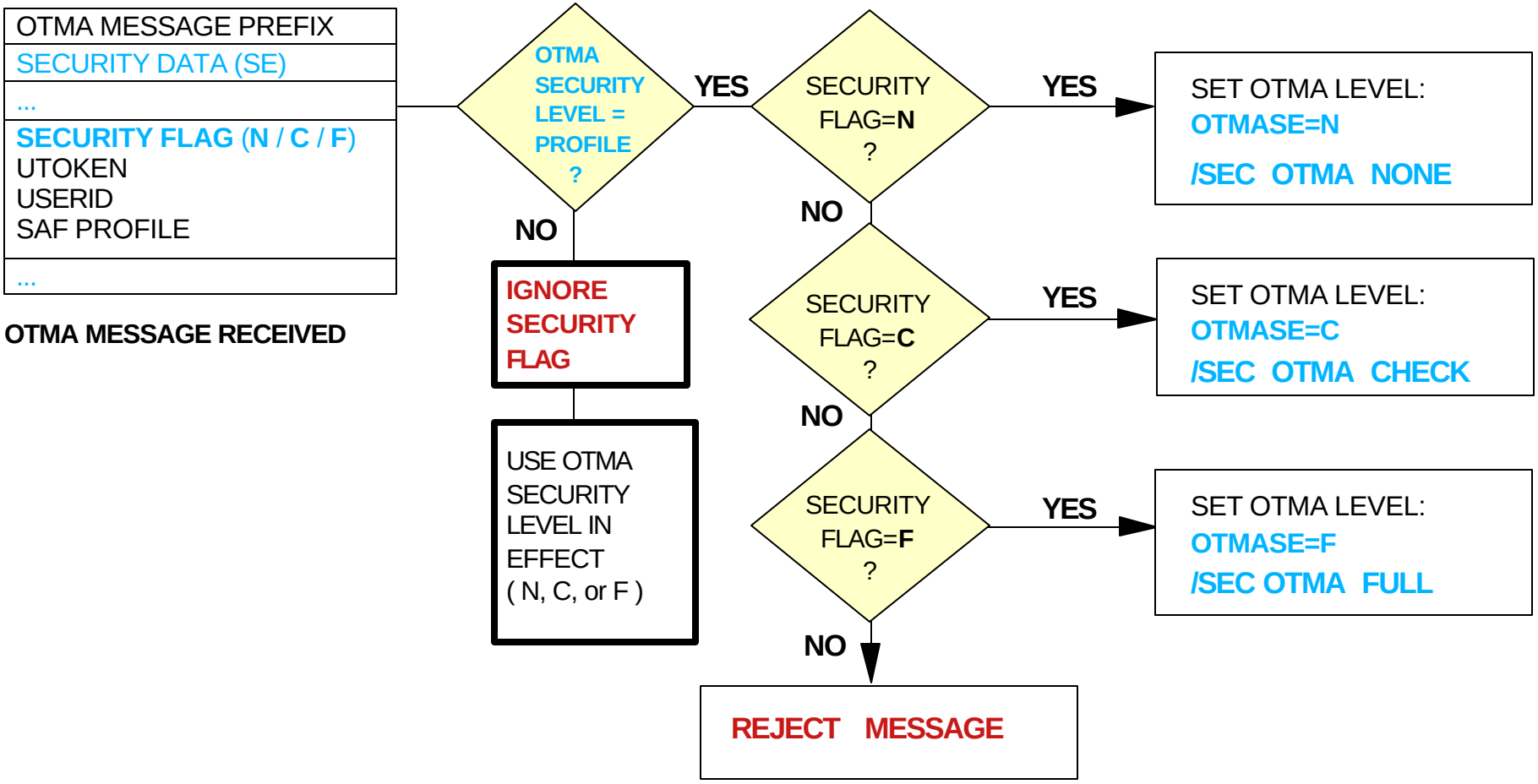
For End User Transaction Messages



OTMA Security Level PROFILE

- With OTMA security level PROFILE
  - Security checking is done on a ***message-by-message*** level rather than an ***IMS-wide*** level
    - For all client-bid and end user messages
    - This provides ***flexibility*** for varying security requirements
- Considerations for using PROFILE
  - The 1-byte security flag in the OTMA prefix may be set by
    - The application ***programmer*** that creates the message
    - The OTMA client
  - Security flag is used by OTMA ***only*** when the OTMA security level is PROFILE
    - The security flag is not used when the OTMA security level is NONE, CHECK, or FULL

PROFILE Logic Flow



EXIT IS INVOKED -or- EXIT MAY BE INVOKED

DFSCCMD0, DFSCTRN0, and DFSCTSE0

OTMA Callable Interface (OTMA C/I)

- OTMA C/I
  - Introduced in IMS V6 via APARs PQ17203 and PQ32398
    - Requires OS/390 V1R3 or higher
  - Application programming interface that may be used to access IMS from C/C++ applications on z/OS or OS/390
  - Support is provided for
    - Authorized programs
      - ***Client-bid security*** is ***not*** performed for ***authorized callers*** (e.g. WebSphere for z/OS) which use the API
    - Unauthorized programs
      - ***Client-bid security*** ***is*** performed for ***unauthorized callers*** which use the API (e.g. user written C/C++ application running on z/OS)
      - Security provided by RACF and ' ***IMSXCF.OTMACI*** ' FACILITY class profile
        - Userid of program must have **READ** access level or higher
  - Does ***not support*** OTMA security level **PROFILE**

Summary

- OTMA overview
- OTMA security overview
  - IMS/OTMA security levels
    - IMS/OTMA security enhancements
  - OTMA Callable Interface (OTMA/CI)
- Additional information
- Summary
- For your information, the following have also been included
  - Where to go for additional information
  - Explanation of acronyms used in the presentation
  - RACF examples
  - Customers that helped define and/or test the new OTMA security enhancements

Additional Information

'*OTMA Guide and Reference*' manual

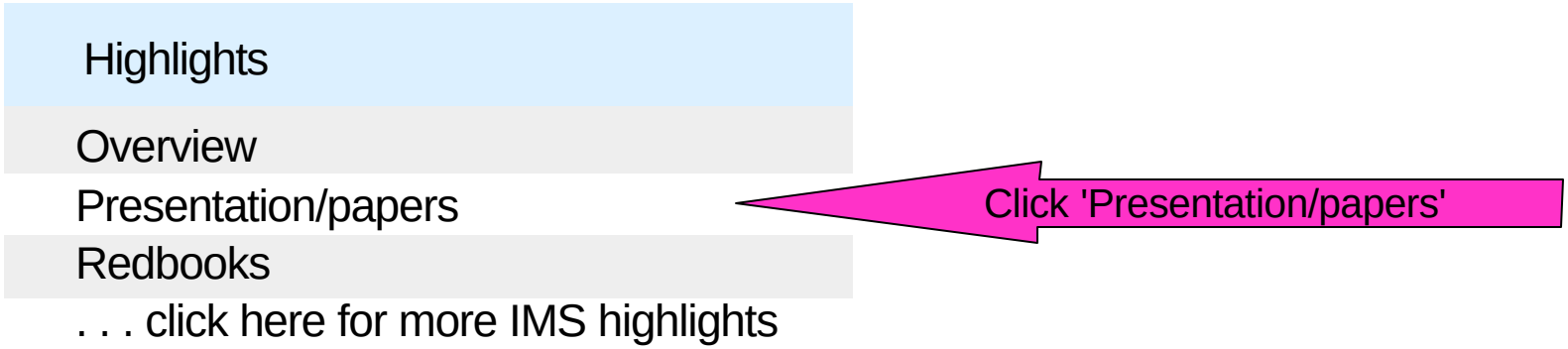
'*Security Options and Considerations*'

Abstract: A white paper detailing the security options for IMS/Open Transaction Manager
(OTMA), IMS Connect, and the MQSeries-IMS Bridge Application

WEB sites

Exact page: http://www-3.ibm.com/software/data/ims/shelf/presentations/

From IMS home page: http://www-3.ibm.com/software/data/ims/



Acronyms

- Cross-System Coupling Facility **(XCF)**
- Information Management System (IMS)
  - Open Transaction Manager Access **(OTMA)**
  - Open Transaction Manager Access Callable Interface **(OTMACI)**
- WebSphere-MQ for OS/390 or WebSphere-MQ for z/OS **(MQSeries)**
- Multiple Virtual Systems **Sys**tems Com**plex** **(MVS SYSPLEX)**
- Operating System/390 **(OS/390)**
- Resource Access Control Facility (**RACF)**
- System Authorization Facility **(SAF)**
- Transmission Control Protocol/Internet Protocol **(TCP/IP)**
- Virtual Telecommunications Access Method **(VTAM)**
- zSeries/Operating System **(z/OS)**

RACF Command Examples

- Sample RACF commands are shown to secure
  - The ***client-bid*** process

For OTMA client subsystems (i.e. IMS Connect and WebSphere-MQ)

```
RDEFINE IMSXCF.XCFGRP1.HWSMEM UACC(NONE)
PERMIT IMSXCF.XCFGRP1.HWSMEM CLASS(FACILITY) ID(HWS1PROD) ACCESS(READ)

RDEFINE IMSXCF.XCFGRP1.CSQ1PMEM UACC(NONE)
PERMIT IMSXCF.XCFGRP1.CSQ1PMEM CLASS(FACILITY) ID(CSQ1PROD) ACCESS(READ)
RDEFINE IMSXCF.XCFGRP1.IMS1MEM UACC(NONE)
PERMIT IMSXCF.XCFGRP1.IMS1MEM CLASS(FACILITY) ID(CSQ1PROD) ACCESS(READ)
```

IMS CONNECT

MQ-IMS BRIDGE

Non-authorized programs using the OTMA callable interface

```
RDEFINE IMSXCF.OTMACI UACC(NONE)
PERMIT IMSXCF.OTMACI CLASS(FACILITY) ID(PGMAUSID) ACCESS(READ)
```

UNAUTHORIZED PROGRAM USING OTMA C/I

RACF Command Examples ...

- Sample RACF commands are shown to secure
  - ***IMS commands*** entered by end users

```
RDEFINE CIMS DBR OWNER(IMSADMIN) UACC(NONE)
PERMIT DBR CLASS(CIMS) ID(GROUPX DBAGROUP OTMAUSRS) ACCESS(READ)

RDEF DIMS IMSUSER ADDMEM(DIS STA) OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSUSER CLASS(DIMS)  ACCESS(READ) ID(GROUPY OTMAUSRS APPCUSRS)
```

  - ***IMS transactions*** entered by end users

```
RDEFINE TIMS TRANA  UACC(NONE)
PERMIT TRANA CLASS(TIMS) ID(OTMAUSRS APPCUSRS GROUPX) ACCESS(READ)

RDEFINE GIMS PAYTRANS  ADDMEM(PAYRAISE,PAYDECR,PAYROLL) UACC(NONE)
PERMIT PAYTRANS CLASS(GIMS)  ID(GROUPY  OTMAUSRS) ACCESS(READ)
```

Special Thanks To ...

- Customers
  - **Steve Nathan,** Telcordia
  - **Dave Cameron,** Royal Bank of Canada
    Ralph Spadafora, Royal Bank of Canada
    Greg Ross, Royal Bank of Canada
  - **Wang Chen,** Toronto Dominion Bank
  - **Jean Rollet**, AGF-French Insurance Group
  - Bank One, John Deere, Verizon, USAA, and others

- IBM
  - **Bob Gilliam**, Silicon Valley Lab, IMS Family Product Manager
    - **Jack Yuan**, Silicon Valley Lab, IMS Developer
    - **Gerald Hughes**, Silicon Valley Lab, IMS Developer and IMS Connect Developer
  - **Suzie Wendler and Lonnie Coleman**, IMS Advanced Technical Support, Dallas, Texas

RETURN TO INDEX